UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,581	12/20/2001	Joseph M. Fontana	2356P	3274

7590 05/25/2004

SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER	
ELISCA, PIERRE E	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,581	FONTANA ET AL.	
	Examiner	Art Unit	
	Pierre E. Elisca	3621	MW

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-17,20-22,24-26 and 29-39* is/are rejected.

7)☒ Claim(s) *4,5,18,19,23,27 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 1/4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to Applicant's amendment, filed on 3/15/2004.

2. Claims 1-39 are presented for examination.

CLAIM OBJECTION

3. Claims 4, 5, 18, 19, 23, 27, and 28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102 (b)

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 (b) that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 6-17, 20-22, 24-26 and 29-42 are rejected under 35 U.S.C. 102 (b) as being anticipated by Takenaka et al (U.S. Pat. No. 5,917,908).

As per claims 1, 3, 12, 16, 17, 20, 21, 22 and 39-42 Takenaka discloses a file protection system for protecting a file which is stored in a storage unit, comprising:

encrypting the software to be protected using an encryption key, creating encrypted software, wherein the encryption key is derived from a dynamic key, which is assigned

to the software to be protected and does not change between copies of the software (see., abstract,);

in response to the security device being coupled to the computer system, sending information identifying the protected software from the computer system to the security device (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64);

authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software to determine if the dynamic key assigned to the software is present in the security device, and if so, generating the encryption key within the security device using the dynamic key (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64); and

authorizing use of the software on the computer system by sending the encryption key from the security device to the computer system for decryption of the software (see., abstract, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key). Takenaka discloses using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information are readable as first and second keys, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key). Takenaka discloses the claimed method of using an initialization vector (or first key) and a dynamic key or second key as the first and second pieces of information (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5,

lines 6-67, col 9, lines 19-64, ID or encryption key or code). Takenaka discloses the claimed method of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract). Takenaka discloses the software package has been loaded on the computer (see., abstract). Takenaka further discloses a random number on the computer system (see., col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64, please note that random number is readable as a pseudorandom number generator, and the authentication program see., abstract, software algorithm).

As per claim 2 Takenaka discloses the claimed method of using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information is readable as first and second keys);
associating the first piece of information (or first key) with the encrypted software (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64); and
storing the second piece of information (or second key) in the security device (see., abstract, specifically wherein it is stated that a second key (or second piece of information), external to the software, to be protected which bears a relationship to the first key, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claim 3, Takenaka discloses the claimed method of sending the first piece information associated with the encrypted software to the security device (see., abstract, specifically wherein it is stated that an algorithm for processing a plurality of

keys including the first key (or first information) in software, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64); and

using the first piece of information and the second piece of information to generate the encryption key in the security device (see., abstract, please note that first and second pieces of information is readable as first and second key, and the first and second keys in the algorithm for deriving a control key, please note that the control key (control key or encryption key) is for decrypting the software, and also col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claims 6, 13, 14, 15 and 20 Takenaka discloses the claimed method of using an initialization vector (or first key) and a dynamic key or second key as the first and second pieces of information (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claim 7, Takenaka discloses the claimed method of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract).

As per claim 8, Takenaka discloses the claimed method of embedding a mathematical algorithm (fig 1, item 16, col 3, lines 23-39, mathematical algorithm or algorithm) within the security device to create the communication key (or proper key) and the security key (or newly control key) from the dynamic key (or second key) and the initialization vector

or first key (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claim 9, Takenaka discloses the claimed method of including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processor (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claim 10, Takenaka discloses the claimed method of sharing memory between the security processor and the co-processor and decrypting the encrypted software in the shared memory (see., col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64, please note that the second key can be used to decrypt data in the shared memory since it is a part of the control key).

As per claim 11, Takenaka discloses the claimed method of preventing the software from running in any of the co-processor unless the software has first been decrypted by the security processor (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64).

As per claims 24, 27, 35 and 39 Takenaka discloses the claimed limitations of protecting computer software from unauthorized users, comprising:

encrypting the software to be protected using an encryption key, creating encrypted software (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, col 9, lines 19-64, please note that first and second pieces of information are readable as first and second keys, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are part of the control key);

authorizing use of the software on the computer system by generating the encryption key within the security device using information supplied from the software (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67); and

sending the encryption key from the security device to the computer system for decryption of the software (see., Fig 1, specifically wherein it is stated that the first and second keys in the algorithm for deriving a control key, please note that the control key is for decrypting the software since it is a part of the second key, and also col 1, lines 7-25). Takenaka discloses wherein said initialization vector (or first key) is created from a checksum of encrypted software to be protected (see., algorithm software, abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, ID or encryption key or code). Takenaka further discloses decrypting the encrypted first encryption key on the computer using the second key included in the software (see., abstract please note that the control key is for decrypting the software since it is a part of the second key, and also, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67, it is inherent to recognize that the first key can be used to encrypt data and the second key can also be used to decrypt data since they are parts of the control key).

As per claim 25, Takenaka discloses the claimed limitations using at least first and second pieces of information to generate an encryption key (see., abstract, please note that first and second pieces of information is readable as first and second keys);

associating the first piece of information (or first key) with the encrypted software (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67); and

storing the second piece of information (or second key) in the security device (see., abstract, specifically wherein it is stated that a second key (or second piece of information), external to the software, to be protected which bears a relationship to the first key, col 2, lines 31-54).

As per claim 26, Takenaka discloses the claimed limitations of sending the first piece information associated with the encrypted software to the security device (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67); and

using the first piece of information and the second piece of information to generate the encryption key in the security device (see., abstract, please note that first and second pieces of information is readable as first and second key, and the first and second keys in the algorithm for deriving a control key, please note that the control key (control key or encryption key) is for decrypting the software, and also col 1, lines 7-25, Fig 1).

As per claims 29, 36, 37 and 38 Takenaka discloses the claimed limitations of using an initialization vector (or first key) and a dynamic key or second key as the first and

second pieces of information (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67).

As per claim 30, Takenaka discloses the claimed limitations of using a security key as the encryption key (or control key) and a communications key as the second encryption key (see., abstract).

As per claim 31, Takenaka discloses the claimed method of embedding a mathematical algorithm (abstract, encryption key)

As per claim 32, Takenaka discloses the claimed method of including the encrypted software with an authentication program, wherein the authentication program is embedded within a separate security processor provided in conjunction with the co-processor (see., abstract, col 2, lines 7-67, col 3, lines 1-53, col 5, lines 6-67).

As per claim 33, Takenaka discloses the claimed method of sharing memory between the security processor and the co-processor and decrypting the encrypted software in the shared memory (see., Fig 1, abstract, col 2, lines 7-67, col 3, lines 1-53).

As per claim 34, Takenaka discloses the claimed method of preventing the software from running in any of the co-processor unless the software has first been decrypted by

the security processor (see., abstract, col 3, lines 1-53, col 5, lines 6-67, col 7, lines 34-67).

RESPONSE TO ARGUMENTS

6. Applicant's arguments filed on 3/15/2004 have been fully considered but they are moot in view of new ground (s) of rejection.

Conclusion

7. Applicant's submission of an information disclosure statement under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p) on 3/15/2004 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609(B)(2)(i). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pierre E. Elisca whose telephone number is 703 305-3987. The examiner can normally be reached on 6:30 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703 305-9769. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pierre Eddy Elisca

Primary Patent Examiner

May 25, 2004